STATEMENT OF SENATOR ERNEST F. HOLLINGS
HEARING ON INTERNET SECURITY/HACKING
MARCH 9, 2000

Senator Burns, thank you for holding this hearing today. It is the first hearing in a series that the Committee intends to hold on the subject of electronic privacy.

Internet security and hacking are not generally discussed in the context of privacy, but I think that this is an important first topic for consideration. No matter what we decide on the right policy to protect consumers on the Internet is, no policy can work without a secure infrastructure. A company can have the strongest privacy policy in the world, but that policy is irrelevant if the company has not adequately protected its systems from illegitimate users.

A month ago at this time, Mr. Misener=s company, among others, was under attack. That attack highlighted problems which have plagued the users of the Internet for some time. Having been brought under the media spotlight the question now is: how can we be sure that the companies we are doing business with on the Internet are

secure? Additionally, what do businesses owe their consumers when they are victims of computer break in?

In order to make consumer information safe from hackers, it will be necessary to raise the security standards of Internet-based businesses as a whole. As we try to craft public policy in this area, we need to examine three

constructive roles for government: (1) fostering constructive partnerships which enhance private sector security; (2) pushing the technological envelope on information infrastructure protection; and (3) being a role model through the implementation of best security practices.

In other words, the government must be prepared to form a partnership with industry to share information on new attacks and how to stop them. Our research agencies must invest in solving problems which will bolster the security of the whole Internet rather than its parts. Finally, the government needs to do a better job of protecting its own information. Right now, our departments and agencies are far from a shining example of what Internet security can be. We need to have in place the right policies, hardware, software, and trained personnel to secure government computer systems. I hope that our witnesses will address these areas in their testimony today.

Already, various agencies of the Department of Commerce are doing important computer security work. Undersecretary Reinsch oversees the Critical Infrastructure Assurance Office (CIAO) which is coordinating partnerships with the private sector to examine attack prevention. The National Institute of Standards and Technology (NIST) is a leader in computer security research and, through the 1987 Computer Security Act, sets standards for securing unclassified government computer systems. The FY 2001 budget request for information security would enhance these capabilities at Department of Commerce and in other agencies of government.

Again, I look forward to hearing the testimony of today=s witnesses on how we can improve Internet security in this nation and what the role of the

government should be in achieving that goal.